User Manual

visual iFO Key

Enterprise Edition

SFR IT-ENGINEERING

www.sfr-software.com

September 2005

Contents

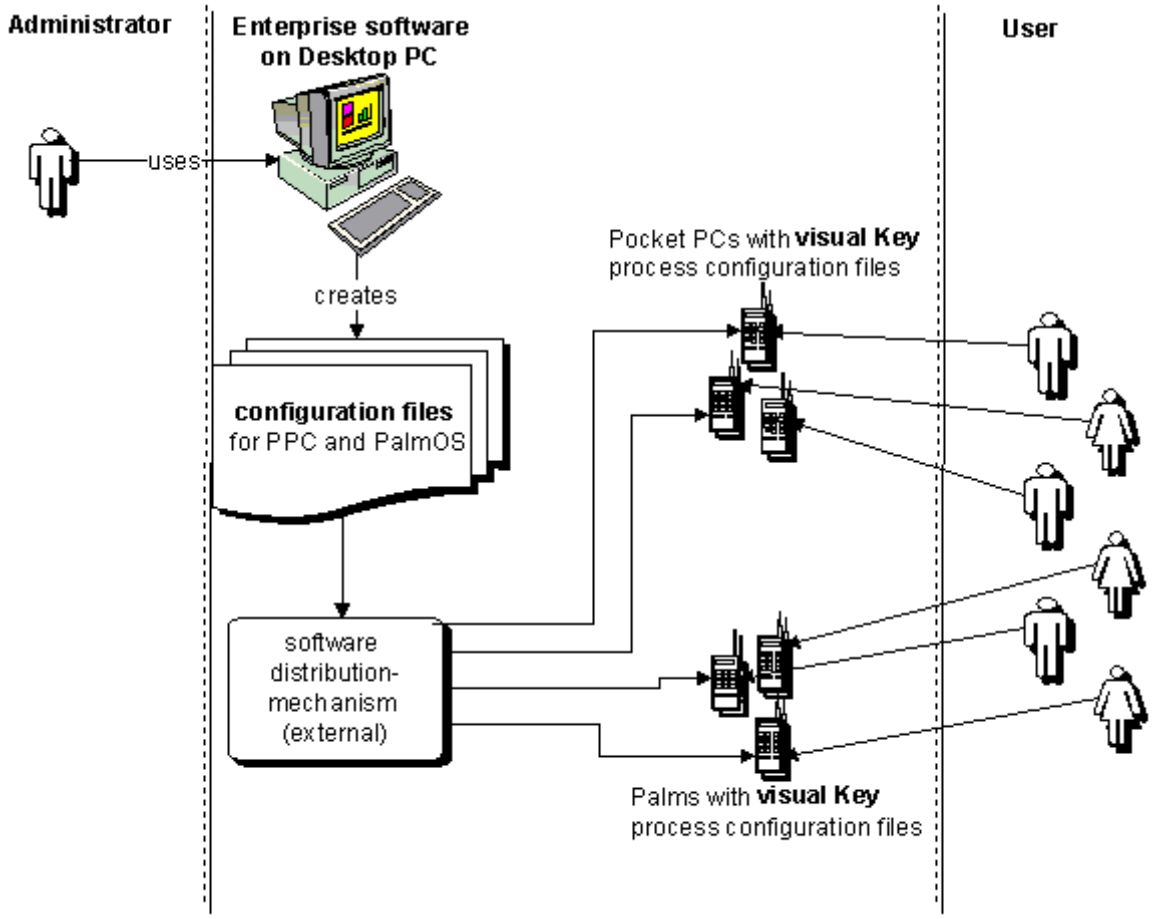
Contents 2
Introduction 4
Installation of visKey Enterprise Edition 5
Starting the administration software 5
Installation of the PDA software 5
Creating configuration files with visKey EE 6
Administrator settings 6
Administrator password 7
Registration 7
Security policies 7
Change password at next login 7
User may select another picture 7
User may deactivate password 7
User may change password 8
User may enter ‚options' screen 8
Duration of password validity (days) 8
Min. length of password 8
Select a picture (visKey Palm OS and Pocket PC) 8
File options 8
Settings for visKey PalmOS 9
Use system password after 3. failure 10
Lock device 10
Power off and lock with pen 10
Input precision 10
Show time 10
Click hint 10
Fast login 10
Backlight 11
Owner info 11
Click sound 11
Fullscreen 11
Hide alarms 11

Voice memo 11
Settings for visKey Pocket PC 12
Hotsync password 12
Hotsync password: Use on power on 12
Input precision 12
Lock device 12
Show date 12
Show text password 13
Show time 13
Owner info 13
Show click hint 13
Play click sound 13
Fast login 13
Fullscreen 13
Create configuration file (visKey Palm OS and Pocket PC) 13
Define the password 14
What to do, if a user is locked out? 15
The patented visual Key technology 16
visKey: An alternative to text passwords 16
The process 16
Technical implementation 17
License Agreement 19

Introduction

The visKey Enterprise Edition - visKey EE - allows central administration of visKey for PocketPC and PalmOS. This includes the predefinition of visual passwords, the implementation of security policies, and the blocking or unblocking of certain options for the users.

An administrator prepares a configuration file at a desktop PC. Afterwards this file is transferred to all of the company's PDA's (Pocket PC's and/or Palm Handhelds). The software visKey already installed on the PDA's will recognize the file and adopt the contained settings. The following picture illustrates the workflow.



Installation of visKey Enterprise Edition

Starting the administration software

After finishing the setup you will find visKey Enterprise Edition in the start menu at \Programs\sfr\visKey Enterprise Edition. A link to the software should also have been created at the Windows desktop.

Installation of the PDA software

There are two ways to install visKey on the PDA's:

1. The administrator or the user copies the needed files to the PDA manually and starts the installation.
2. The administrator uses an external (third party) software distribution mechanism, that installs the files from a central service point to all devices.

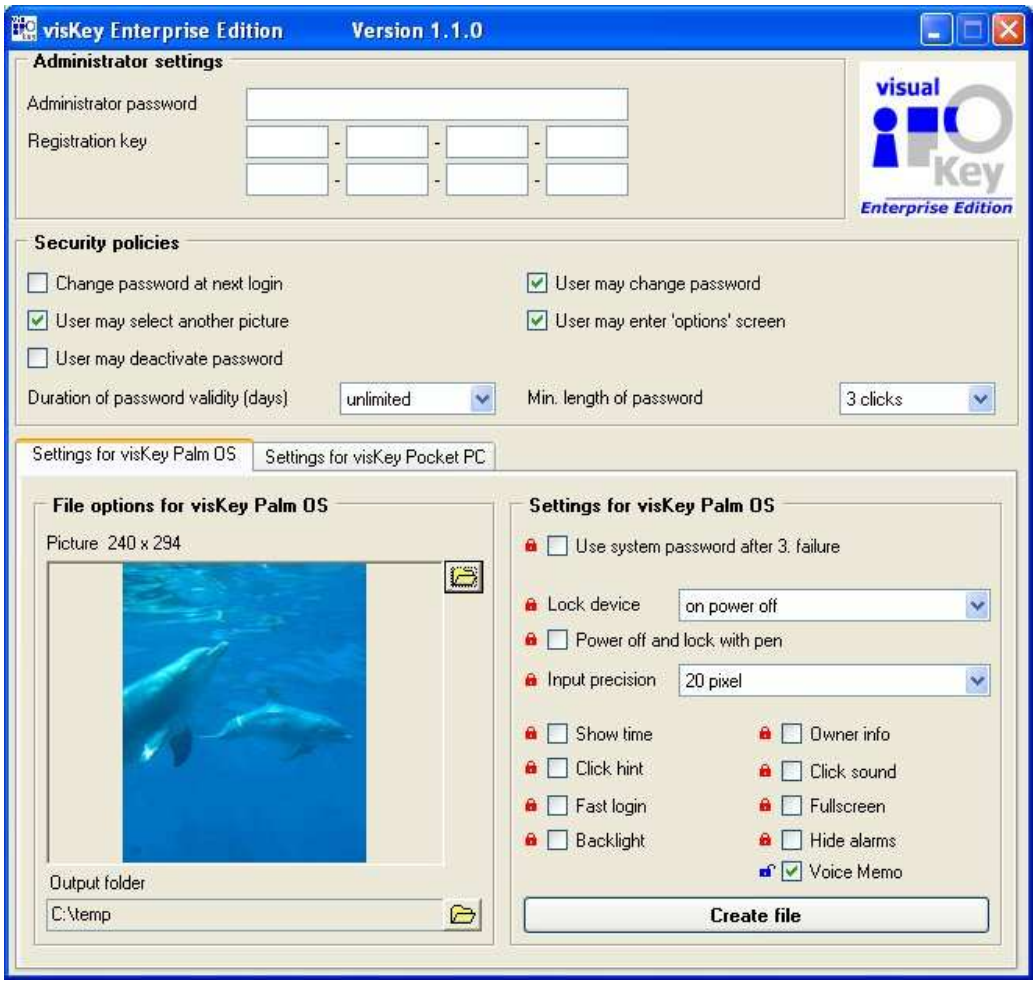
There are three PRC files for visKey PalmOS, which have to be copied to the Palm PDA's.

For automatic configuration with the administrator settings the configuration file has to be created and distributed. This topic is handled in the next chapters of this manual.

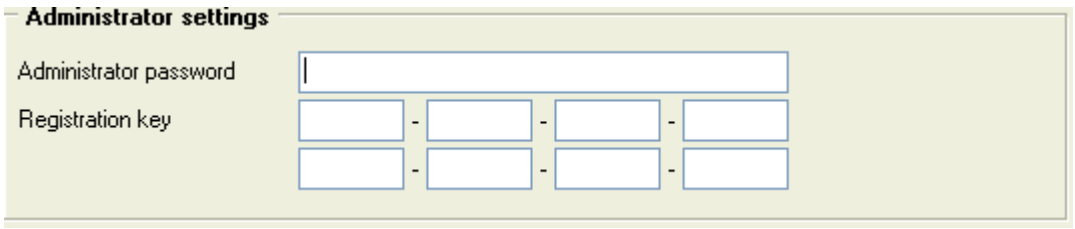
For visKey PocketPC there are CAB files which can be copied to the devices. If you start the CAB file on the PDA, the installation of the software is done.

Creating configuration files with visKey EE

The administration screen of visKey Enterprise Edition contains all necessary settings for predefinition of passwords and settings for the PDA's.



Administrator settings



Administrator password

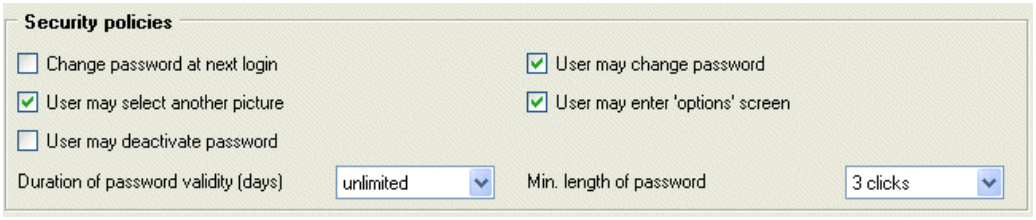
Here you can enter a alphanumeric password which is the master password for all your PDA's with visKey, that have the configuration file installed. You can only enter this password at the PDA's after a soft reset.

Registration

Please enter the registration key, that you have received from SFR to use this administration software. You can see additional information on your licence, after you have entered the registration key.

Security policies

With the security policies in visKey Enterprise Edition company wide restrictions for IT security and password protection can be implemented on all PDA's. The administrator can guide the users to more sensitivity with security and passwords aspects.



Change password at next login

Activating this setting forces the user to define a new password, after the configuration file has been processed by visKey omn the device.

User may select another picture

Activating this setting allows the user to select a new picture, when defining a new password. This setting is only usable in combination with 'User may change password'.

User may deactivate password

Activating this setting allows the user to deactivate the password mechanism in visKey, so he does not have to login at start up.

User may change password

Activating this setting allows the user to change to password. This setting is activated automatically, if you select 'User may select another picture'.

User may enter ‚options' screen

Activating this setting allows the user to enter the options screen in visKey to change settings, which are left usable by the administrator's configuration.

Duration of password validity (days)

Here you can set, how long a defined password is valid. After this time period the user must define a new password.

Min. length of password

Here you can set, how many clicks (minimum) a password must consists of. The 'length' of the password is determining, how secure your password is:

If you have a picture size of 240 x 294 pixels and an input precision of 20 pixels and you have a password with three clicks, you get almost 5 million combinations. With four clicks even 800 million!

Select a picture (visKey Palm OS and Pocket PC)

File options

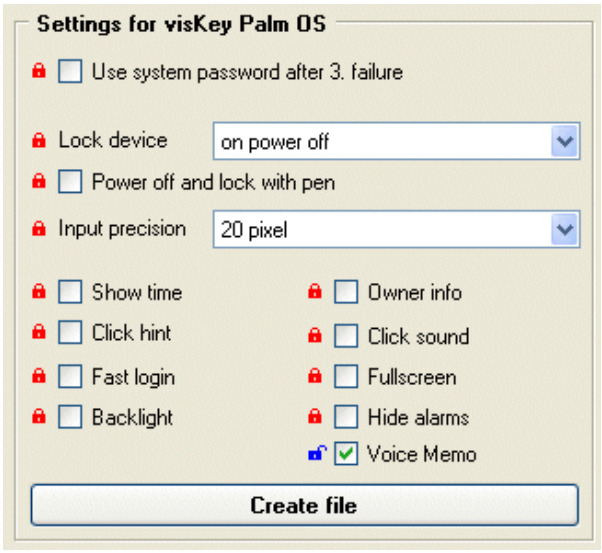
If you click the button near the picture, a dialog appears to select a picture of your choice for your password. You can see a preview of the picture after selection.

Please keep in mind the resolution of your PDA devices. If the size of the picture exceeds the screen of the PDA, you get scrollbars to reach any point on the picture.

The output folder is the folder, where the created configuration files und installation files are stored. The PRC files are for the Palm devices and the VKE files and CAB files are for Pocket PC's. You can change the folder to your preferred destination.

Settings for visKey PalmOS

All security related settings for your Palm devices can be made here. You can lock specific options for the user, so he can't change them on his device. If the 'lock' symbol is open, the user may change this setting on his device.



Use system password after 3. failure

If this setting is activated, the user can use this password to login after the third login failure. This may be necessary in case of decalibration or if the users has forgotten his visual password.

Lock device

This setting contains the duration of inactivity, after which the device is being locked by the system. The option 'with pen' enables the user to use visKey without an automatic lock, but to lock the device manually with a pen stroke from bottom to top of the screen.

Power off and lock with pen

This option enables the user to use visKey without an automatic lock, but to lock the device manually with a pen stroke from bottom to top of the screen.

Input precision

This setting defines the sensitivity of visKey, on how precise the user has to click the previously defined spots in the picture, so visKey recognizes his input as the correct password. Higher values are easier to use and smaller values are more secure.

Show time

Activating this setting allows the user to see the current time on the login screen.

Click hint

Activating this setting allows the user to see the position and number of the current clicks, that he is doing on the picture.

Fast login

Activating this setting allows the user to login to the device after the last correct click without confirming his input with 'OK'. This setting is comfortable but reduces security.

© 2005 SFR GmbH, Cologne, Germany

Backlight

Activating this setting turns the backlight on at several old colour Palm devices (e.g. Palm m505). This option should be deactivated on newer Palms.

Owner info

Activating this setting to enabled the user to view the devices internal 'owner information' with name and address data of the user and/or company. These data can be set in the system options (owner) of each Palm device.

Click sound

Activating this setting enables the Palm to play a sound, when the user is clicking on the picture.

Fullscreen

Activating this setting disables the menu bar in visKey, so the whole screen is reserved for the picture. This setting is only usable in combination with 'Fast login'.

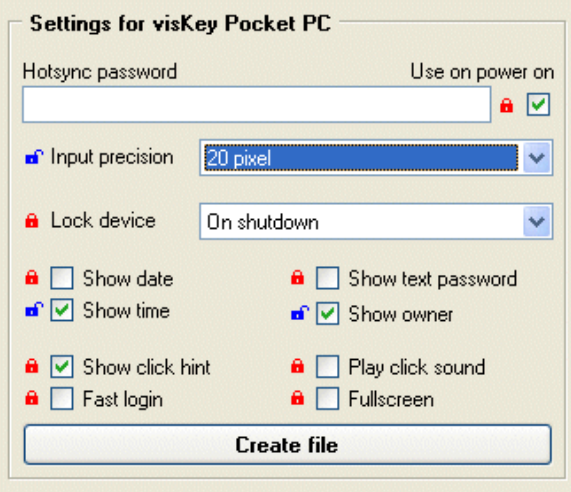
Hide alarms

Activating this setting hides the text of an alarm, until the user has logged in to the device.

Voice memo

Activating this setting allows the user to use the voice memo recorder on the Palm without having to login first. We recommend to deactivate this setting, because switching to another application, while locked, is reduces security.

Settings for visKey Pocket PC



Hotsync password

Define an alphanumeric password here, that the user can use to login to the PPC from ActiveSync software on his desktop PC.

Hotsync password: Use on power on

Enable this setting to allow the user to login via ActiveSync, even if the device itself is still locked by visKey. If this setting is active the user has to login at the device first and then login at ActiveSync. Using this option reduces security, because the hotsync password normally is not as safe as the visKey password.

Input precision

This setting defines the sensitivity of visKey, on how precise the user has to click the previously defined spots in the picture, so visKey recognizes his input as the correct password. Higher values are easier to use and smaller values are more secure.

Lock device

This setting contains the duration of inactivity, after which the device is being locked by the system.

Show date

Activating this setting enables the user to see the current date on the PPC's screen without logging in to the device.

Show text password

Activating this setting enables the user to see the generated visKey password. Administrators should deactivate an lock this option for enterprise use.

Show time

Activating this setting enables the user to see the current time on the PPC's screen without logging in to the device.

Owner info

Activating this setting enables the user to see the owner information of the device, which can be entered in the system settings of the device.

Show click hint

Activating this setting allows the user to see the position and number of the current clicks, that he is doing on the picture.

Play click sound

Activating this setting enables the PPC to play a sound, when the user is clicking on the picture.

Fast login

Activating this setting allows the user to login to the device after the last correct click without confirming his input with 'OK'. This setting is comfortable but reduces security.

Fullscreen

Activating this setting disables the menu bar in visKey, so the whole screen is reserved for the picture. This setting is only usable in combination with 'Fast login'.

Create configuration file (visKey Palm OS and Pocket PC)

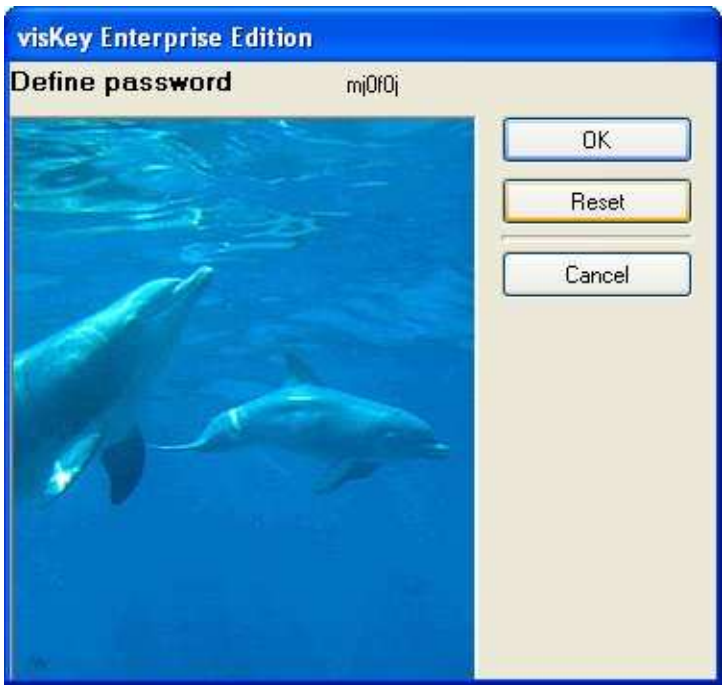
After selection of the picture and setting the output folder for the configuration file you can click on the button 'Create file'.

Then you have to define the new password by clicking several spots in the picture. The password and all settings you have made are stored in the configuration file, which the has to be transmitted to the devices.

The configuration files are

1. 'visKey Settings.prc' (for PalmOS devices)
2. 'visKey Settings PalmOS35.prc' (for older Palm devices)
3. 'visKeyPPC.vke' (for PocketPC devices).

Define the password



To define the password simply click on several significant spots in the picture. Click 'OK' to go on to confirmation or 'Reset' to define another password. After confirmation the configuration files are created and stored in the output folder.

The password can consist of up to eight spots in the picture. Be sure to select at least three different points to gain a 'good' password.

What to do, if a user is locked out?

If a user has locked himself out of the device, the administrator can reactivate the device with his administrator password.

The administrator must do a soft reset of the device and enter his password at the prompt. Afterwards the device is unlocked and the administrator should leave visKey and install a new configuration file on the device to activate the standard settings and password.

The patented visual Key technology

Most operating systems and many programs require, that the user identifies himself. Usually this is effected by typing in a text password. For security reasons these passwords should not be created associatively (NOT the children's first names, NOT the wedding day, etc.). Furthermore, the passwords should be changed regularly.

Thus most computer users have to memorize several difficult and ever changing passwords. This results in severe safety gaps, as many users either ignore these rules or note their passwords down.

visKey: An alternative to text passwords

The disadvantages sketched above may be eliminated in an economical and uncomplicated way by the use of passwords based on images. It is much easier for humans to remember pictures (or parts of pictures) than text. Furthermore, associations with pictures are more variegated and individual.

The input of a visual password is effected by selecting several spots in an image (e.g. by tapping with the stylus). There are more advantages to this method:

- This procedure is not limited to systems equipped with keyboards but may also be employed on touch screens or kiosk systems.
- In comparison to other methods, such as biometric identification technologies, generally no additional hardware is required to employ it, since virtually all today's computer systems are equipped with a mouse or other input device.
- Contrary to biometric identification technologies, there ist no direct correlation between the identification and the person identifying. Several persons may even use the same password.

The process

As a first step to define a password the user chooses an image. This may be any picture, but ideally it should have a multitude of distinguishable details. Then the user selects one or more spots in the picture by stylus tap or using another input device. The password (the visual key) will be created from the selected points and their order.

The chosen details and their sequence are easy to remember. Additionally, the picture itself helps the user to form individual associations ("there is a BOAT on the RIVER, passing a MAN wearing a HAT").

In order to identify himself to the system later on, the user just has to pick the selected spots in their original order in the given picture.

Technical implementation

Before generating the password the program divides the selected picture (not necessarily visible to the user) into cells. The number of created cells forms the maximum character set (the "alphabet") for the password, each cell representing a single character.

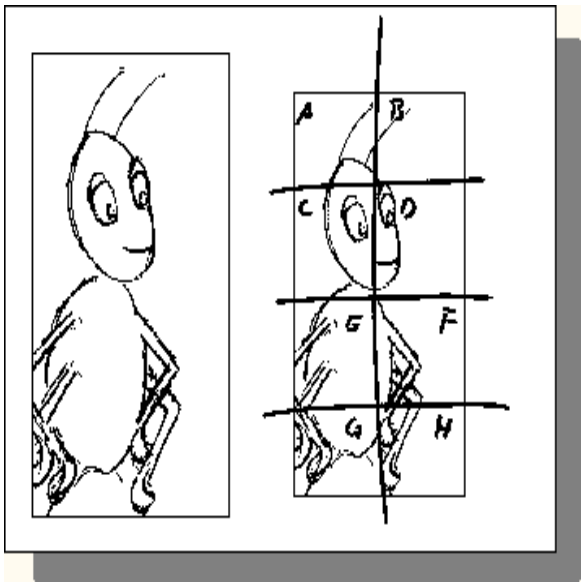
In order to define a password, the user may select any desired spots in the picture: The character of the cell belonging to the spot will be transferred to the password.

Later on, the user identifies himself by choosing the same order of points, thus composing the same password again.

There are two different procedures to divide the image into cells:

1. Regular allocation

The image is divided into regularly sized cells (e.g. rectangles or hexagons). When defining a password this grid is shifted with each input so that any selected spot is situated exactly in the center of a cell. This serves to compensate the inevitable "fuzziness" of later input.



Since it is as good as impossible to hit exactly the same spots (pixels) again when entering the password, this shifting of the entire grid defines the whole cell as valid input area, thus permitting small deviations in any direction.

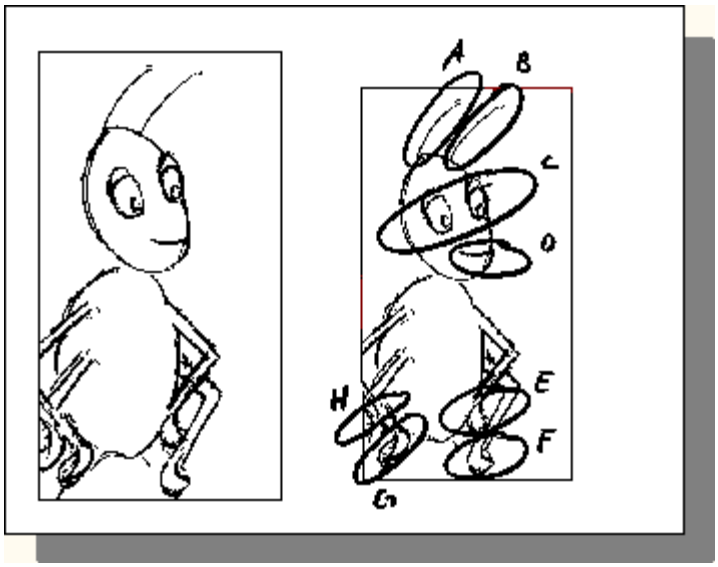
Apart from the graphic, the cell size and the offsets of all grid shifts must be stored. All this information will be needed to generate the correct password from the user's input. However, it is neither necessary nor wanted to store the password itself.

The security of the password depends on the cell size as well as on the width and height of the underlying graphic, since these data determine the total number of cells and thus the range of the alphabet.

The regular allocation procedure is used by visKey. Additionally, for each touch the first cell's value is randomized and stored. Thus the first cell does not always represent the character "A" but may contain any character.

2. Irregular allocation

With the irregular allocation of a graphic its particularities can be taken into account (distinct points, individual symbols, remarkable areas). In this case the allocation is done either manually or with appropriately "intelligent" programs. In contrast to the first procedure there is no unspecific fault tolerance. Therefore the user and the creator of the mask have to agree upon how certain symbols shall be analyzed (e.g. "edge or surface").



In addition to the graphic the complete mask (the alphabet) must be stored. Again the security level of the password is dependent on the range of the alphabet (total number of defined areas).

This procedure is currently not supported by our visKey products but may be subject to future enhancements.

License Agreement

visKey Enterprise Edition

Version 1.1.0

Copyright © 2005 SFR Gesellschaft für Datenverarbeitung mbH, Cologne, Germany

All Rights Reserved

Please read the following terms and conditions before using visKey Enterprise Edition. In the event that you use this software, you are agreeing to be bound by the terms and conditions of this agreement. Should you not agree with these terms, do not use visKey Enterprise Edition.

SFR grants you an exclusive and not transferable license to use visKey Enterprise Edition on the contracted amount of PCs and PDA's. Copy's for backup purposes are allowed.

COPYRIGHT

The software visKey Enterprise Edition and the documentation are owned by SFR and are protected by copyright laws and international treaty provisions. No title to intellectual property is being transferred. You may not modify, reverse engineer, decompile or disassemble the software. You may not translate, reverse engineer, decompile, disassemble, modify or patch the visKey Enterprise Edition executable files or documentation in any way.

LIMITED WARRANTY

SFR warrants that the program will perform in substantial compliance with the

documentation supplied with the software product. If a significant defect in the product is found, the Purchaser may return the product for a refund. In no event will such a refund exceed the purchase price of the product.

Limitation of Liability: EXCEPT AS PROVIDED ABOVE, YOU AGREE THAT SFR SHALL NOT BE LIABLE, UNDER ANY LEGAL THEORY, INCLUDING TORT, CONTRACT OR OTHERWISE, FOR ANY DAMAGES INCURRED BY YOU INCLUDING BUT NOT LIMITED TO DIRECT OR INDIRECT DAMAGES FOR LOSS OF GOODWILL, LOSS OF DATA, BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR OTHER COMMERCIAL OR PECUNIARY LOSS, ANY CONSEQUENTIAL, SPECIAL OR INCIDENTAL DAMAGE) OR ANY OTHER PERSON OR ENTITY AS A RESULT OF YOUR USE OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION EVEN IF SFR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF

INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

GENERAL

This Agreement is the entire agreement between SFR and you, supersedes any other agreements or discussions, oral or written, and may not be changed except by written amendment signed by the author of this product. This Agreement shall be governed by and construed in accordance with the laws of Federal Republic of Germany, excluding its conflict of laws, rules and the United Nations Convention on Contracts for the International Sale of Goods. If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal or unenforceable, such provision shall be severed from this Agreement and the other provisions shall remain in full force and effect.

Should you have any questions concerning this license agreement, or if you desire to contact SFR for any reason please e-mail SFR at enterprise@sfr-software.com.